What Is Claimed Is:

1. A method for electronically signing a message in a cellular phone (60), comprising the following method steps:
generating an electronic fingerprint from the message to be signed, in a personal computer (10);
transmitting the electronic fingerprint from the personal computer (10) via a communications network (110) to any cellular phone (60) which contains a signing device;
signing the received electronic fingerprint in the cellular phone (60); and
retransmitting the signed electronic fingerprint to the personal computer (10).

2. The method for electronically signing as recited in Claim 1,
wherein a secret key can be stored in the cellular phone (60), and a public key, assigned to the secret key, can be stored in the personal computer (10),
the electronic fingerprint is signed using the secret key in the cellular phone (60) and is retransmitted to the personal computer (10), and
the signed electronic fingerprint is converted using the public key into an unencrypted electronic fingerprint which is compared to the electronic fingerprint generated from the message to be signed.

3. The method for electronically signing as recited in Claim 1 or 2,
wherein the electronic fingerprint is generated in accordance with a hash function from the message to be signed.

4. The method for electronically signing as recited in one of Claims 1 through 3,
wherein the electronic fingerprints are transmitted between the cellular phone and the personal computer using an SMS, e-mail or WAP service.

5. A communication system, in particular for implementing the method for electronically signing as recited in one of Claims 1 through 4, which comprises:
at least one personal computer (10) that is able to be linked to a communications network (110), as well as at least one cellular phone (60) assigned to the communications network,
the personal computer (10) containing a device (40) for generating an electronic fingerprint from a message to be signed, as well as a transmitting/receiving device (20) for transmitting the electronic fingerprint to any cellular phone (60), and
the cellular phone (60) having a receiving device (70) for receiving an electronic fingerprint transmitted by the personal computer (10) via the communications network (110), a signing device (90) for signing the received electronic fingerprint, as well as a transmitting device (70) for retransmitting the signed electronic fingerprint to the personal computer (10).

6. The communication system as recited in Claim 5, wherein the cellular phone (60) has a memory (80) for storing a secret key, and the personal computer (10) has a first memory (32) for storing a public key assigned to the secret key,
in addition, the personal computer (10) having a device (40) for converting a received, signed electronic fingerprint using the public key, as well as a comparator (50) for comparing the converted electronic fingerprint to the electronic fingerprint generated from the message to be signed.

7. The communication system as recited in Claim 5 or 6, wherein the personal computer (10) has a second memory (38) for storing software which enables the personal computer to communicate with the cellular phone (60).

8. The communication system as recited in one of Claims 5 through 7,
characterized by a third memory (30) in which the call numbers of at least one cellular phone and/or a target device (100) are able to be stored, and by a device (40) for automatically dialing a cellular phone and/or a target device.